The Ollila Law Group LLC
2060 Broadway
Suite 300
Boulder, Colorado 80302

PATENT APPLICATION

ATTORNEY DOCKET NO. 35010/097

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Allan L. Samson et al.

Application No.: 09/489,864 **Group No.:** 2434

Filed: 01/24/2000 **Examiner:** Simitoski, Michael J.

For: SYSTEM FOR PREVENTING TAMPERING WITH SIGNAL CONDITIONER REMOTE FROM A HOST SYSTEM

MAIL STOP APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P. O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR REHEARING

Introduction

A notice of appeal was filed on September 7, 2004 and an appeal brief was filed on November 1, 2004. An appeal decision was mailed on October 29, 2008, affirming the 35 U.S.C. 102 and 103 rejections of the final Office Action.

Pursuant to the provisions of 37 CFR § 41.31 *et seq.*, Applicants hereby request a rehearing on the record regarding the decision on appeal to the Board of Patent Appeals and Interferences (the "Board"). Applicants are entitled to a Rehearing per 37 CFR 41.52. Applicants have two (2) months in which to file the Request for Rehearing. 37 CFR 41.52(a)(1). The Request for Rehearing must state with particularity the points believed to have been misapprehended or overlooked by the Board.

Applicants file this Request for Rehearing within the two month deadline of December 29, 2008.

It is believed that no fees are due at this time. However, if it is determined that fees are due, the Commissioner is authorized to debit Deposit Account No. 502622 for the required fees.

Summary of Errors of Fact:

A) The Board's decision erroneously does not define or correctly interpret authentication information.

B) The Board's decision erroneously asserts that the patent specification does not include express definition of the terms tampering, authentication, and signal a tampering condition.

C) The Board's decision erroneously asserts that Lumsden would not process data from a transponder that did not match an identification or authentication comparison and some indication/signal should then be generated by the host system.

D) The Board's decision erroneously asserts that the transponder identification of Lumsden comprises authentication data.

E) The Board's decision erroneously asserts that Lumsden uses the transponder identification to determine tampering within the signal conditioning circuitry.

F) The Board's decision erroneously asserts that if there is a discrepancy between the data received from the transponder to the information stored at the central computer, an error may be deemed to have occurred.

A) Error of Fact: The Board's decision erroneously does not define or correctly interpret authentication information.

The Board appears to view any data as authentication data. This is an incorrect interpretation of the meaning of authentication information.

Authentication information is information that can change, but is not authorized to be changed by others, except by the manufacturer or agents thereof (see page 2, lines 15-22 and lines 28-33). An unauthorized change in the authentication information is tampering. This can include a change performed in order to adjust a measurement or output of the system (see page 8,

lines 19-23).

The specification clearly defines the authentication information, stating that the signal conditioner stores "calibration and configuration data as well as a unique identification" (see page 3, lines 16-20). The specification further states that "the identification, calibration, and configuration data are termed authentication data." Such identification, calibration, and configuration information is understood by one of skill in the art to be information intended to not be changed except by the manufacturer or qualified service personnel. The authentication information is further understood by one of skill in the art to be information that would not be externally known or easily discoverable, as it might be used to control the generation of measurement data (see page 3, lines 31-33, and page 6, lines 17-21 of the present application).

Lumsden does not disclose calibration and configuration data. Lumsden discloses that "[e]ach transponder, at the time of its installation, has **hard wired** therein an identification code. The [transponder] microprocessor, upon receipt of an instruction word set compares the second word with the code **hard wired** therein . . ." (see col. 2, lines 48-50 of Lumsden)(emphasis added). The transponder identification code of Lumsden therefore cannot be changed.

Lumsden further includes a customer identifier (see col. 3, lines 9-22). Lumsden discloses that the customer identification code is "**permanently stored**" in a transponder (see col. 8, lines 60-62). The customer identification code of Lumsden therefore cannot be changed. Consequently, by definition, neither the transponder identification nor the customer identification comprises authentication information for at least the reasons stated above. Further, the transponder identifier of Lumsden is not used for authentication in an authentication process.

B) Error of Fact: On page 9, line 21 to page 10, line 2 of the Board's opinion, the Board states that the patent specification does not include express definition of the terms "tampering," "authentication" [*i.e.*, an authentication process], and "signal a tampering condition" and further asserts that "[f]inding no express definitions in the Specification and Appellants have not identified any specialized interpretation based upon the disclosure or the pertinent prior art, we give these terms there [sic] broadest reasonable ordinary and customary meanings, and find that the teachings of Lumsden are clearly within the broadest reasonable

interpretation."

The Board misapprehended the definitions contained in the text of the patent application.

The tampering, authentication process, and resulting signaling are clearly outlined in the patent application.

An **authentication process** is understood by one of skill in the art to be the comparison of authentication data in order to detect a change in the data. An authentication process according to page 7, lines 26-30 of the specification discloses that "[a] tamper proof system . . . stores a record of authentication data transmitted to the host system 100 from the signal conditioner 100 to ensure that someone does not tamper with signal conditioner 110. The authentication information is checked periodically to insure against tampering". More specifically, an authentication process comprises comparing a known good authentication information (the initial information) to the received authentication information, received from the signal conditioner (see page 3, lines 27-29).

Lumsden does not disclose an authorization process. Lumsden does not disclose comparing known good authentication information to received authentication information. The transponder identification of Lumsden is alleged to be authentication information. However, Lumsden divulges that the transponder identification is hard wired and is therefore not changeable. It is built into the transponder. A comparison therefore would not detect a change in a transponder identifier of a particular transponder unit. A comparison in Lumsden will only determine which transponder is communicating.

Not only is an authentication comparison not disclosed in Lumsden, but there is no disclosure in Lumsden of what may occur as a result of a comparison failure; let alone any determination of tampering. Therefore, the interpretation of a transponder identifier as being authentication information, used in an authentication process, is erroneous and not reasonable.

Tampering is clearly outlined in the patent application. Page 2, lines 15-22, and page 8, lines 19-23 of the present specification makes clear that tampering comprises someone other than a manufacturer or agent changing the authentication information (compare page 2, line 15, "manufacturers", with line 17, "prevents others from changing calibration information . . ."). The specification and claims illustrate that the host system stores initial authentication

information for a signal conditioner (see page 4, lines 20-26) and subsequently detects a tampering occurrence by requesting the authentication information from the signal conditioner (see page 4, line 31 to page 5, line 2) and then compares the received authentication information to the stored initial authentication information (see page 4, lines 27-29). A tampering signal is generated if the received authentication information does not match the initial authentication information.

In the past, tampering prevention has included physically blocking or making physically apparent any access to a signal conditioner after manufacturing has been completed, wherein tampering is imputed from such (improper) access (see page 2, lines 15-22). In the past, tampering prevention has included maintaining an audit trail of information likely to be tampered with, wherein tampering would be evident from changes in any of the information stored in the audit trail over time (see page 2, lines 28-33).

The process of **signaling a tampering condition** is clearly outlined in the patent application. Page 8, lines 19-23, would be understood by one of skill in the art to be the process of signaling a tampering condition, where the signaling would not occur unless the received authentication information does not match the initial authentication information. The signaling occurs after a comparison failure.

With regard to signaling a tampering condition, Lumsden simply does not discuss processing or handling an error condition. Lumsden therefore *cannot* discuss signaling an error condition. Lumsden does not discuss comparing initial and received authentication information in order to determine if the authentication information has changed in an unauthorized manner.

The Board's decision proposes that a transponder identification comparison comprises detecting tampering. It is clear that the transponder identifier is not used to identify tampering. It can be seen, from context, that the transponder identifier of Lumsden is merely used for addressing/message routing (see col. 2, lines 50-56). There is no discussion in Lumsden of a transponder identifier being used to "signal a tampering condition in the signal conditioning circuitry in response to said authentication information not being equal to said initial information" or equivalent.

The final rejection proposes that a comparison of electrical consumption measurements

comprises detecting tampering.

A person of skill in the art would not view a comparison of message addresses or a comparison of time-varying measurement data to be any form of tampering detection. Tampering with the transponder ID of Lumsden would NOT generate erroneous measurements. Lumsden does not teach or suggest detecting tampering with a transponder identifier. Lumsden does not teach or suggest detecting tampering in a transponder unit.

C) Error of Fact: On page 9, lines 14-16 of the Board's opinion, the Board states that "Lumsden would not process data from a transponder that did not match an identification or authentication comparison and some indication/signal should then be generated by the host system." The BPAI decision makes the statement that "[a]t column 6, lines 42-45, Lumsden teaches that specific circuitry is built into the system to test the quality of the received message to insure that it has been correctly sent, received, and decoded."

The point misapprehended or overlooked by the Board is in equating signal quality in communications to be tampering or error detection.

While Lumsden does teach "specific circuitry is built into the system to test the quality of the received message to insure that it has been correctly sent, received, and decoded," it is an enormous leap in logic, unsupported anywhere in Lumsden, that sending and receiving messages would therefore include **or** require that Lumsden perform a testing of data in a message for any tampering in the transponder unit sending the message. Quality in message transmission refers to signal strength, noise levels, and other factors that degrade message reception.

Lumsden does not teach or suggest not processing received data, as is erroneously asserted by the Board. There is no citation to back up this assertion. The stated non-processing does not exist and the Board is improperly implying actions that Lumsden does not include. This violates the "all elements" rule and renders the concept of prior art to be all-inclusive. The Board cannot read features or actions into the prior art.

D) Error of Fact: On page 8, line 26 to page 9, line 1 of the Board's opinion, the Board holds the "transponder identification data [of Lumsden] to be authentication data . . . ." On page

8, lines 20-26 of the Board's opinion, the Board states that "Lumsden discloses that a central computer scans all transponders every 30 seconds" and notes that "[e]ach transponder, at the time of installation, has an identification code hardwired therein to assist in a low probability of error in the transmission of instructions and data. Each time the central computer communicates with an individual transponder, the transponder identification is included and each response thereto similarly contains the transponder identification."

The point misapprehended by the Board is that the transponder identification/identifier of Lumsden is not authentication data, as in the present claims.

The transponder identifier is not equivalent to the authentication information, as was refuted in the appeal brief at page 12, second full paragraph.

The transponder identifier comprises an address or identifier that is used for establishing communication and routing messages (see col. 2, lines 39-43 and lines 48-59; see claim 3). The central computer in Lumsden broadcasts a message to ALL transponders over a telephone line or radio link. A transponder uses the embedded identifier in order to decide whether to accept the message (see col. 2, lines 50-53). The identified transponder, according to the embedded transponder identifier, will be the only transponder to accept the message (see col. 6, lines 49-67; see col. 23, lines 25-32). The comparison, and any error detection, is performed by the individual transponder (see col. 2, lines 48-53).

Lumsden does not teach or suggest that the central computer performs error detection using the transponder identifier. The central computer may perform typical communication error checking, such as by using the parity bit in the first message word (see col. 9, lines 3-5) or by employing a "noise error detection circuit 111" (see FIG. 3), but the transponder identifier of Lumsden is not authentication data. Lumsden does not teach or suggest "authentication" according to the process in the present claims. Lumsden does not describe the transponder identifier as being used for any manner of authentication process or purpose. The Board's decision does not cite any portion of Lumsden that could reasonably be relied on for holding that Lumsden performs any manner of "authentication" process on message data.

It is known in the art to use message identifiers/addresses in order to detect transmission errors. However, the cited passage of Lumsden, stating that "to ensure a low probability of error

in the receipt of instruction data sets and the transmission of data word sets", is clearly referring to message routing and the detection errors during transmission, and NOT errors in the data due to tampering that may have occurred before transmission.

The Board did not note or correct the Examiner's assertion of the transponder identifier being equivalent to the authentication information. Instead, the Board appeared to be signaling implicit agreement with the Examiner.

The Examiner argued that the claim element of "signaling a tampering condition" was shown in Lumsden by the action of issuing a "load shed instruction/alarm/condition" (see final Office Action, page 10, under the "response to applicant's arguments" heading) and asserted this was further shown by Lumsden signaling "a tampering condition/load shed . . . ***in response to*** said authentication information/word set not being equal to said initial information" (see page 4 of the Examiner's Answer)(emphasis added). This last statement is an amalgamation of unrelated pieces of Lumsden, as the load shedding action has no relation to the transponder identifier or customer identifier. Therefore, the assertion of "in response to" is wholly fictitious. The load shedding of Lumsden occurs when the electrical provider determines that a user is consuming excessive electrical power, such as during a peak usage period, and can send a message or command that impacts electrical power provision (see col. 1, lines 22-38). Lumsden's stated purpose is to notify consumers of excessive electrical power consumption during peak hours and optionally perform load shedding (see col. 1, lines 15-42). Lumsden states that "[t]he next step in moderating power consumption is for the utility to be able to shut off non-essential loads in the consumer's home when the power consumption for a given time period approaches a predetermined level. A particular embodiment of the present invention is capable of performing this load shedding function upon receipt of the correct coded message from a central computer." (see col. 1, lines 39-42). The Examiner's Answer conflates the two actions: 1) the comparing of a received transponder identifier to a stored transponder identifier, with 2) the signaling of a load shedding condition. The Examiner's Answer improperly links the two separate actions into a tampering detection action.

Further, the electrical power consumption of a utility customer is an authorized action, as customers are allowed to consume power. Determining a load shedding action is not equivalent

to detecting tampering. Such an assertion is unreasonable and violates the commonly accepted meaning of the term tampering. Further, the load shedding determination will be based on a threshold that is set by the utility, and not based on a transponder/customer identifier mismatch.

E) Error of Fact: On page 9, lines 2-9 of the Board's opinion, the Board states that "the use of the identification code can represent a tampering within the signal conditioning circuitry wherein if the signal conditioning circuitry has the wrong identification code, this would identify a possible tampering with the signal conditioning circuitry by the response to the central computer having the wrong transponder identification code." The Board further states that the "central computer then compares the authentication information with initial information which is stored at the central computer about the totality of all the transponder units."

The point misapprehended by the Board is that the transponder identification of Lumsden is not being used to detect tampering.

This was refuted in the appeal brief at page 11, bottom of the first full paragraph.

The Board's decision erroneously assumes that: 1) the central computer is configured to perform a tampering comparison, 2) the transponder identifier is authentication data, 3) a transponder identifier could be changed in an unauthorized manner, 4) changing a transponder identifier would be of benefit to a person doing the tampering, and 5) the central computer signals some manner of tampering error condition if the received transponder identifier does not match any stored transponder identifier. Lumsden does not teach any of these points, let alone all of them.

As discussed above, Lumsden does not teach or suggest detecting any unauthorized changes to a transponder identifier. Lumsden instead indicates that a transponder identifier is used for addressing and routing messages, as is done in the art (see col. 2, line 39 to col. 3, line 31). Tampering with the transponder ID of Lumsden would NOT generate erroneous measurements. Lumsden does not teach or suggest detecting tampering with a transponder identifier. Lumsden does not teach or suggest detecting tampering in a transponder unit.

Lumsden does not discuss any actions taken, or signals generated, if a received transponder identifier fails a comparison in the central computer.

The Examiner's Answer varies by page and shifts between data elements of Lumsden, as if the Examiner is merely guessing and does not fully comprehend the reference. For example, in the paragraph at the bottom of page 7, the Examiner implies that electrical power measurements are being compared to "initial data" in the form of a power consumption threshold. However, at page 8, last paragraph, the Examiner's Answer states that 1) ". . . Lumsden discloses an error condition/load shed command indicating possible tampering . . . in response to authentication [sic] information/word set (col. 8, line 54 – col. 9, line 6) not being equal to the initial information (col. 4, lines 35-40)." The cited text at col. 8, line 54 to col. 9, line 6 of Lumsden concerns the transmission of a message from a transponder unit to the central computer and the transponder identification code and the customer identification code, while the cited text at col. 4, lines 35-40 concerns load shedding and an electrical consumption quota. The Examiner's Answer therefore considers the transponder identifier to be equivalent to the authentication data and yet considers the power consumption measurement data to be equivalent to the authentication data.

This inconsistency is outlined at page 11, lines 23-28 and at page 12, lines 3-6, of the appeal brief.

The electrical power consumption measurement data of Lumsden comprises a changeable measurement quantity. The data cannot be employed in a comparison action in order to detect a change, as the measurement quantity is certain to change over time. Further, the final Office Action ignores the fact that the stored threshold is not an initial form of the power measurement and the stored consumption threshold is likely set by the utility. The stored consumption threshold might vary by consumer, by region, by time of day, et cetera.

F) Error of Fact: On page 9, lines 9-11 of the Board's opinion, the Board states that " [i]f there is any discrepancy between the data received from the transponder to the information stored at the central computer, an error may be deemed to have occurred."

The point misapprehended or overlooked by the Board is that Lumsden does not disclose detecting or processing an error.

Lumsden does not state OR imply this. The above statement in the Board's decision is

without basis in fact. No citation is provided to back up this assertion. The above statement cannot be found in Lumsden.

Lumsden may compare a received transponder identifier with a list of known transponders in order to identify the transmitting transponder unit. Lumsden states that "[t]he microprocessor [of the transponder], upon receipt of an instruction word set compares the second word [*i.e.*, the transponder identifier] with the code hard wired therein and accepts the instruction word set if and only if the identification words coincide." (see col. 2, lines 50-53). However, Lumsden does not discuss or even suggest any actions to be taken if the comparison does not produce a match, such as where a received transponder identifier is unknown. A lack of a match could be attributed to various faults, including poor transmission conditions or an out of range problem, such as where the system of Lumsden is using a disclosed radio link instead of a telephone land line. Because the central computer in Lumsden is using public telephone lines or public radio spectrum to communicate with transponders, the result of no match is that a received message with an unknown transponder identifier (or format unknown to the central computer) would merely be ignored by the central computer. There is NO suggestion of such a comparison and subsequent error decision action in Lumsden.

The only occurrences of the term "error" in the text of Lumsden are at col. 2, line 39; col. 3, line 31; and col. 10, line 3. The text of Lumsden does not include the term "discrepancy". The text of Lumsden includes the terms "comparison" and "compare" in claim 1, referring to the comparison of a transponder identifier for addressing purposes, and at col. 2, line 51; at col. 8, line 50; and at col. 9, lines 28, 32, 35, and 40.

CONCLUSION

In view of the above, applicant respectfully request that the examiner's rejection of claims 1-12, 15-20, 23-30, and 34-44 be reversed.

Respectfully submitted,

Date: 12/16/08

SIGNATURE OF PRACTITIONER

Gregg Jansen, Reg. No. 46,799
Ollila Law Group LLC
Telephone: (303) 938-9999 ext. 14
Facsimile: (303) 938-9995

Correspondence Address: Customer No: 32827